

VU Research Portal

IT enabled risk management for taxation and customs: the case of AEO assessment in the Netherlands

Liu, J.; Burgemeestre, C.B.; Hulstijn, J.; Tan, Y.H.

published in

Lecture Notes in Computer Science
2009

DOI (link to publisher)

[10.1007/978-3-642-03516-6_32](https://doi.org/10.1007/978-3-642-03516-6_32)

document version

Publisher's PDF, also known as Version of record

[Link to publication in VU Research Portal](#)

citation for published version (APA)

Liu, J., Burgemeestre, C. B., Hulstijn, J., & Tan, Y. H. (2009). IT enabled risk management for taxation and customs: the case of AEO assessment in the Netherlands. *Lecture Notes in Computer Science*, 5693, 376-387. https://doi.org/10.1007/978-3-642-03516-6_32

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

E-mail address:

vuresearchportal.ub@vu.nl

IT Enabled Risk Management for Taxation and Customs: The Case of AEO Assessment in the Netherlands

Jianwei Liu¹, Yao-Hua Tan^{1, 2}, and Joris Hulstijn¹

¹ Vrije Universiteit Amsterdam, Faculty of Economics and Business Administration,
Information Systems Group, 1081 HV Amsterdam, the Netherlands

² Technical University Delft, Dept. of Technology, Policy and Management
jliu@feweb.vu.nl, ytan@feweb.vu.nl, jhulstijn@feweb.vu.nl

Abstract. Building collaborative relationships with trusted businesses is a long-term strategy for EU governments. Recently, for the EU Tax and Customs Administration (TCA), the realization of this goal has become more visible with the emerging concept of the Authorized Economic Operator (AEO). Businesses in the member states can apply for the AEO certificate. When it is being granted, simplified control procedures and trade facilitation will be provided by the TCA. A possible “win-win situation” can be achieved, with increased trade efficiency and lowered administrative burden. However, without proper selection of trusted business partners, governments may be worse off due to the adverse selection problem caused by information asymmetry. In this paper, we analyze the cause and effect of the adverse selection in the Government-to-Business relationship building. Further, we show that an IT enabled risk assessment approach can effectively eliminate the G2B information asymmetry and solve the adverse selection problem. The AEO assessment approach of DutchTCA is analysed to give a real life application on how IT is enabling the general risk management approach of the DutchTCA.

Keywords: G2B relationship building, adverse selection, risk management, AEO.

1 Introduction

One of the key visions for e-government is to enhance government relationship with businesses and citizens: turning a government service into a self-service, for better participation, enhanced efficiency and lowered administrative burden. Tax and Customs administrations facing the challenge of growing trade volumes and increased security requirements are now adopting this vision, by applying advanced information technology (IT) to achieve the objective of building new collaborative relationships with businesses. The collaborative relationship means to change the G2B relationship from the traditional “control and command” to a more “trust-based” relationship, which includes replacing the traditional labour intensive customs controls with businesses’ “self-control” regarding to customs issues. To realize this transformation, the EU Directorate-General of Tax and Customs has made a major effort to develop and promote the concept of the Authorized Economic Operator (AEO) for European

businesses [1]. The underlying idea is that if businesses can prove to the TCA that they are in control of the tax and security aspects of their own business processes, then they will be AEO certified by the TCA, which brings them the benefits of less physical inspections, fast customs clearance procedures and trade facilitation by the TCA. The aim is to achieve a win-win situation for both government and businesses, with trade simplification and lowered administrative burden.

However, because businesses typically have better information about themselves than the government (information asymmetry), problems of *moral hazard* and *adverse selection* may occur. Moral hazard means that businesses tend to act opportunistically and inappropriately; adverse selection means that good companies are driven out of the market by bad ones (For details see, [2], [3] and [4]). In Section 2, we investigate how adverse selection may have a negative effect on the AEO certification process in the sense that, due to information asymmetry between the government and businesses, the government can be misled, and will certify companies that are actually not in control. If this happens, the good companies who are in control will perceive this as unfair competition, leave the market, and will no longer apply for the AEO certificate. Hence, a so-called “lemons market” for AEO certificates may be created, which would make the certificate virtually useless. In Section 3, we argue that, by applying an IT enabled risk assessment approach, the adverse selection problem in the AEO certification process can be effectively reduced, enhancing the trust relationship between government and businesses. Businesses can show to the government that they are “in-control” by sending a positive *signal* to the government based on their business information systems and internal control quality. There is also a second role of IT: when businesses use IT enabled decision support systems to perform the AEO self-assessment, the quality of the self-assessment increases, and hence the strength of the positive signal can be further enhanced. Based on this, governments are better able to perform a risk assessment, to *screen* and differentiate trustworthy businesses from opportunistic ones and entitle the AEO certificate only to the good ones. In Section 4, we analyse a case study with DutchTCA of the AEO certification procedure. We analyzed what role IT is playing in the risk management for the AEO assessment. Based on this case study, we provide recommendations for EU policy making on AEO certification.

2 Asymmetric Information in G2B Relationships Forming

To form any kind of relationship, information sharing is essential. In an ideal world we assume information is shared equally and transparently among the parties. However in the real world, due to lack of communication channels and hidden incentives for sharing or hiding information between parties, information is normally spread in an asymmetric way. Information asymmetry occurs when one party has more or better information than the other party. Typically, two problems are triggered by asymmetric information, namely, moral hazard and adverse selection ([2], [3] and [4]).

Moral hazard refers to “situations where one side of the market can’t observe the actions of the other. For this reason it is sometimes called a hidden action problem” [5]. It arises because an individual or institution in a transaction does not bear the full consequences or can hide the consequences of its actions without the counter party knowing it, and therefore has an incentive to act inappropriately. Tax fraud can be seen as a typical moral hazard problem in G2B relationships. For example, in VAT (Value Added Tax)

collection, two parties are involved: a company who is obliged to declare VAT and pay the tax; and a tax office which audits the tax declaration and collects the VAT. Under the assumption of perfect information, the tax office obtains complete information and knows about the company's exact operation; the company reports and pays the correct amount of VAT (Figure 1a). However, in the real world the company has better information about its own operating details than the tax office, and thus may have incentives to hide and even falsify certain information from the tax office to get tax advantages. If such an incentive is present, or the penalty of defaulting is not severe enough, the company might choose tax evasion--- a moral hazard problem is caused (Figure 1b). In a previous paper [6] we have discussed the issues of moral hazard in detail. In this paper we focus on the second problem: adverse selection.

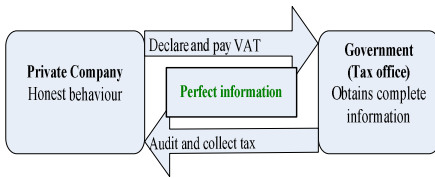


Fig. 1a. Ideal situation (Perfect information)

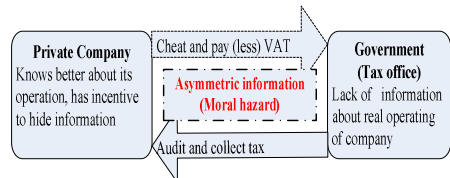


Fig. 1b. Moral hazard (Asymmetric information)

Adverse selection refers to a failing market due to information asymmetries between buyers and sellers, where "bad" products or customers are more likely to be selected rather than the "good" ones. A famous example of adverse selection is illustrated by [2] for the second-hand car market, which is referred to as a "lemon market". Buyers of second-hand cars typically do not have the expertise to know whether a car is a "lemon" (bad car) or a "cherry" (good car), so they are willing to pay an average price that lies in between the lemons and cherries. However, with such a price, the good car dealers are not willing to sell the cars with premium quality. As a result, cars with lower than average quality will be sold: the "cherries" are driven out and "lemons" will dominate the market.

In the G2B relationship, adverse selection can occur when government bodies select private partners and grant certificates. The Authorized Economic Operator (AEO) certificate may serve here as a good example. The idea of AEO is that each EU Member State Customs Administration can establish partnerships with private companies and certify them with the AEO status. The involvement of the companies in AEO will enhance a win-win situation for the safety and security of international trade: on the one hand government can do less physical checks and use limited personnel for other tasks, and on the other hand the certified AEO companies will enjoy tangible benefits such as fast customs clearance and simplified procedures (e.g. containers of AEO companies will not be inspected by the customs when they pass the EU border) [7]. AEO can be seen as an extra Customs control instrument that enhances the Customs control while it does not introduce extra control burden for the government. More specifically, it is a form of government delegating certain control tasks to collaborative businesses and in return giving these businesses trade simplification.

A critical issue here is that the AEO certificate is quite unlike other governmental requirements; it is voluntary rather than mandatory: "It requires ... no obligation for

economic operators to become AEOs, it is a matter of the operators' own choice..." [1]. Companies can make their own decisions on whether or not to qualify for the AEO certificate, based on company strategy. In addition, in spite of the facilitations AEO companies may have, the AEO certificate is not cost free. Companies have to make considerable investments (around 50K euros for small, up to a couple of million euros for large companies) to achieve and maintain the certificate. Hence, we can see AEO as a free will certificate "market", with entry cost and associated benefit.

The problem raised here is that if the government can not effectively differentiate companies from the two streams, a similar adverse selection problem like in the second-hand car market may occur. The "good" (trustworthy and compliant) companies are not willing to join when they see no fair value for them to participate: as one of the interviewed companies (a Netherlands-based international brewery) said "We are already a compliant company with a good reputation, and our current procedure is simpler than that of others anyway, why should we invest more to get the AEO certificate?". On the other hand, the "bad" (opportunistic and fraudulent) companies may see more benefits (less checking and simplified procedure may create an easier way of committing fraud), less cost (they can make a false report to show the fulfilment of the requirements), and thus are more willing to get the certificate (See Figure 2).

The original aim of the government is to focus control effort on potentially fraudulent companies, and limit the number of physical inspections and simplify the procedures for trusted companies with an AEO certificate. As indicated in the interview with the Dutch Tax and Customs Administration (DutchTCA): "If companies are already in good control themselves, why should we waste our resources to exert extra control on them?" However, the consequences of the adverse selection problem may diverge from government's expectation. The situation may even deteriorate, when more "bad" companies obtaining the AEO certificate but committing fraud nevertheless --- a market of "lemons" will be created and the public will lose their trust in the government. Nevertheless, there are remedies for the adverse selection problem. One possible solution is to apply an IT-based risk management approach for effective *signalling* and *screening*, which will be discussed in the next section.

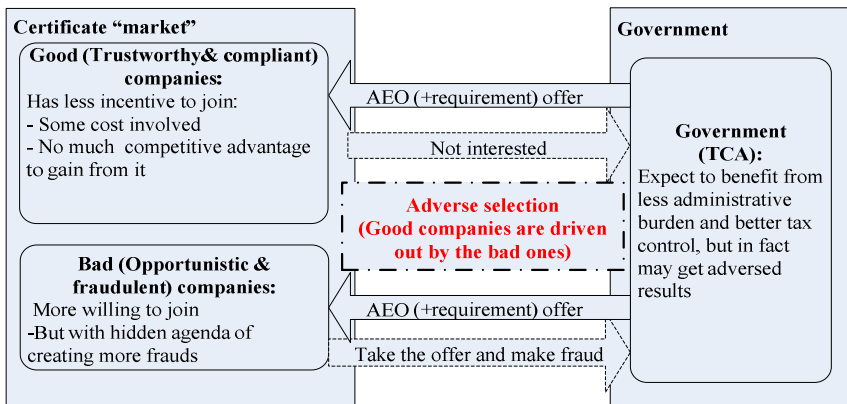


Fig. 2. Adverse selection caused during AEO certification procedure

3 IT-Based Risk Management for Effective Signalling and Screening: The Case of AEO Assessment in the Netherlands

O'Reilly [8] indicates that the quality of decision making increases with the decision maker's information level. However, if the quality of information itself can hardly be evaluated, information behaviour (information seeking and information encountering activities) can have important signalling effects on observers [9]. "*Signalling*" has been considered as one of the most important strategies of solving asymmetric information problems in the job market and capital market, e.g., [3, 10]. The general idea behind signalling is that one party (informed party) conveys some meaningful information (signal) about himself to another party (under-informed party). Due to this extra information, the under-informed party is able to classify the counter parties as good or bad and make sensible selection decisions. "*Screening*" is another way of dealing with adverse selection, but in contrast to signalling, now the under-informed party moves first. It means that the under-informed party can induce the other party to reveal their information, for instance by providing a menu of choices in such a way that the choice depends on the private information of the other party [4]. An example in the job market, a job candidate will send his CV with education level and working experience to the employer to signal that he is the most suitable candidate; at the same time, employers will arrange their own interviews and assessment procedure to screen the candidates and test their abilities.

With our case study, we investigate a possible solution for the AEO adverse selection problem. We undertook in-depth interviews with DTCA on their general AEO assessment approach. Semi-structured interviews were used as the primary method for the data collection [11, 12]. We conducted seven interviews with DutchTCA and attended one auditing visit with DutchTCA to an AEO applicant company. In total we interviewed ten persons from DTCA and three from the company. The interviewees typically have an auditing or EDP auditing background. Interviews were tape recorded with the informants' prior agreement, then transcribed for participant's feedback and our analysis. We discovered that IT-enabled risk management may effectively eliminate the information asymmetry for G2B relationship building. DutchTCA has adopted risk management as part of their audit procedures. They view it "as a structured process, consisting of well-defined steps, according to which a systematic identification, analysis, prioritization and treatment of risks is taking place, so as to support improved decision-making" [13]. The so-called IT-enabled risk management has two meanings: first it means that information technology and information systems are the main focus for the assessment, and second it refers to automated IT support, in the form of decision support systems, for the general risk management approach. In this case, DutchTCA assesses the IT maturity level of the companies, and uses it as one of their major decision criteria for AEO certification. Moreover, DutchTCA deploys as much IT facilitation as possible to make the risk management more efficient and effective. The following major findings were discovered in our case study.

3.1 Finding 1: IT as an Effective Way of Signalling for Businesses

Application of advanced IT may serve as a effective way of signalling for businesses to indicate their types, which will enable the government to effectively differentiate

“good” from “bad” companies for certification. One of the major concerns for the government in the AEO certification is the supply chain safety and security. Gutierrez and Hintza [14] argue that supply chain security can be implemented via facility management, cargo management, human resource management, information management and business network and company management systems. IT facilitation can enhance all five perspectives: 1) for facility management, the use of IT has greatly improved inventory management and control. IT-based access control procedures and technologies (e.g., PKI security, smart cards) enhance facility protection and monitoring functionality; 2) for cargo management, the use of cargo tracking and tracing and anti-tampering technologies (e.g., bar code, RFID, GPS tracking, smart container seals) and cargo inspection technical solutions have enhanced cargo management; 3) for human resource management, most modern organizations apply Enterprise Resource Planning (ERP) system for better HR management, information dissemination and responsibility assignment; 4) for information management system, real time information recording and secure data exchange have been adopted by many organizations; 5) for business network and company management system, most companies have already built up a company security management system and business partner evaluation system for better risk management. IT-based control for supply chain security can significantly lower labour costs and data error rates associated with scanning items and extended identification to individual items. The systems can provide quality information that enables companies to track literally billions of objects across the value chain, increasing the efficiency of individual processes, improving asset utilization, increasing the accuracy of forecasts, and improving the ability of companies to respond to changing conditions of supply and demand [15].

With our case study we find that there are two main signals that a company can send to the government to prove their security status: 1) the use of integrated IT applications for supply chain management (e.g., well implemented ERP system, just-in-time (JIT) programs, electronic data interchange (EDI), and point-of-sale data sharing programs) and, 2) the use of IT applications for security control (e.g., application of GPS, Radio Frequency Identification (RFID) and smart seal technology). To apply for AEO status, companies must first fill in a self-assessment. Part of the self assessment is a risk analysis, detailing the security threats and their impact for a specific company. In addition to the above mentioned general IT systems, companies can also run the self-assessment via an automated toolset, which is yet another enhanced signal to the government. In our case, an automated self-assessment tool “Digiscan”, developed by Deloitte, was used. The Digiscan tool is an expert system that is based on the AEO guidelines and criteria issued by the EU. It is a rule based system, to supports companies to identify in their own organization cases of potential Customs related risks. The system consists of facts, decision rules, and a rule interpreter. All facts are stored in a database and the evaluated risks are described in abstract mathematical rules. A rule consists of one or more facts (preconditions) connected with each other and actions. Rules in the form of IF “x” THEN “y” are particularly suitable. These rules are the basis for the computer-assisted analysis of risk cases. Digiscan supports the company’s AEO self-assessment in an interactive question-answering style. The system generates, based on the AEO Guidelines, a sequence of questions that help the company to improve the quality of their self-assessment. As Digiscan supports a risk based, systematic and objective description of the business, the quality of the business

self-assessment can be perceived better than without it. The end result of the Digiscan supported self-assessment is a so-called summary result which ranks the company on a 1-5 scale for various risk indicators. This summary can be used by DutchTCA for further evaluation. Currently, the value of automated tools to assist in self assessment is under still debate. Potentially, such tools could enhance the reliability of the self assessment. Using the tool would then count as a signal that the company takes compliance seriously. However, the current version of the tool, an automated questionnaire, may not be suited for the purpose of conducting a thorough risk analysis and self assessment. Therefore, DuchtTCA and Deloitte are currently discussing adjustments, both to the tool and to the way its evidence is being used in auditing.

3.2 Finding 2: IT Support for Effective Screening by the Government

Instead of passively receiving “signals” from applicants, DutchTCA also actively *screen* companies by including the specific IT requirements in the AEO selection criteria that all applicants have to fulfil in order to get the certificate. In our research project we discovered in various cases that two principles are essential for explaining the supporting role of IT for AEO self-assessment; namely (1) *Real-Time Monitoring* and (2) *Information Sharing*. **Real-time monitoring** means that IT is used to monitor continuously the location and state of the cargo. For example, in one of the pilot projects that are part of our research project, a smart container seal, TREC (Tamper-Resistant Embedded Controllers), was introduced. The TREC sends information via encrypted GSM or satellite communication about the precise location and unauthorized opening of the container (opening without proper digital certificate). This information is typically received by the owner of the container, or the carrier who is transporting this container. However, when this TREC information can also be shared with the TCAs, the government will have most of the relevant information needed to execute its fiscal and security control tasks. **Information sharing** is done via a service-oriented architecture that gives the DutchTCA direct access to the data bases of the owner and the carrier, to read the stored TREC data about the container.

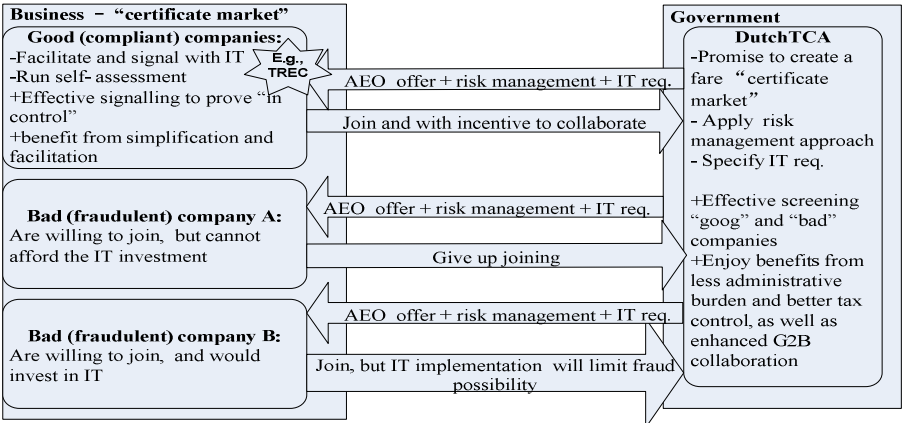


Fig. 3. IT based risk management for AEO certification

Hence, if this type of IT is referred to in the AEO self-assessment of a company, then the government knows that containers from such a company are unlikely to be used to smuggle goods, and hence they do not have to physically inspect these containers at the border. In this way, the right type of IT can support the AEO certification process. DutchDTA will not require specific IT solutions, to avoid being biased towards specific IT vendors, but they could recommend generic types of IT solutions, like smart container seals or service-oriented architectures. With the risk based and IT enabled screening from the government side internal control signalling from the business side, the adverse selection is tackled. Figure 3 presents the changes: for the “bad” company (A), as the signalling costs of implementing the required IT solution will outweigh the potential fraud benefit, he will decide not to apply for the AEO certificate. Anyhow, if the “bad” company (B) would like to have simplified tax and customs procedure and decides to apply for the AEO certificate, he must be compliant with the IT requirements of the government. Moreover, the implementation of the advanced IT solution itself will minimize the fraud possibilities of the “bad” companies and may finally transfer the “bad” companies to “good” ones. The market can correct itself such that “good” companies join and the “bad” ones may leave the market.

3.3 The Role of IT in the DutchTCA AEO Risk Management

It is agreed that a systematic and clear step plan is required for the auditors in the AEO certification process to make an un-biased professional judgment. Our findings from the interviews indicate that DutchTCA mainly relies on a risk management approach for the AEO certification. The purpose of using a risk management approach is to focus customs’ control activities and their limited resources, in particular, on specific risks that are not sufficiently covered by measures taken by the businesses. Therefore, they have to assess the economic operator’s organization, processes, procedures, administration, and so on. The main model used by DutchTCA is the AEO COMPACT Model [16], which requires that the AEO applicants implement, in accordance with their business model and risk analysis, the systems, procedures, conditions and requirements established in the Community Customs Code and the AEO Guidelines [16]. Figure 4 represents the risk management approach, underlying the AEO certification process, which we elicited based on our interviews. We focus on the IT enabled steps (steps with a * sign at the beginning) and skipped the details in rest of the analysis below.

a) **Determine fulfilment of formal (legal) conditions (details skipped)**

As the first step of AEO assessment, DTCA have to determine whether the formal conditions related with the procedure or facilitation for the company is fulfilled. If the applicant cannot fulfill the formal legal conditions, the application will be refused.

b) ***Understand the business (of an operator) through examination of:**

- From Customs internal sources
- ❖ *IT enabler: Primarily based on DutchTCA’s own internal database (National Risk Database) and filing system (RBpro) for effective internal screening.*

The National Risk Database (RDB) is a computerized method for recording and considering risks in the fiscal process. The RDB application is accessible to all staff members of the DutchTCA. In the RDB the whole ‘lifecycle’ of a risk is recorded. After the introduction of the risk, the results of coverage are recorded in RDB in almost the same terms as used during the phase of the preliminary investigations. Every tax official can consult the risk database at any moment to see if a certain risk is already recorded, as well as which risks are recorded in the base.

RBpro is an automated filing system which contains the entire AEO applicant’s existing Customs certificates, basic information of the company and its historical compliance record (e.g., whether the company has violated the law and to which extent); and information can also be retrieved from company historical data profiles gathered in the past through customs import and/or export systems, VAT or other information from the tax services.

- From external sources: via the Internet, companies’ annual financial reports, and auditors report on internal control, etc. and via communication with Chambers of Commerce and Central Statistics (under Dutch law, DTCA has no right accessing it)
- ❖ *IT enabler: Use of XENON web robot for effective external screening*
XENON is a business intelligence software tool, which is used by DutchTCA since 2004. It is an Internet (web) robot, which not only detects unknown tax evaders, but also other probable non-compliant events such as the unauthorized use of brand names or illegal diversion of trade.

c) Clarify the customs’ objectives (details skipped)

- General objectives: are the fiscal as well as the security requirements of the Community Customs Code implemented?
- Specify additional objectives based on the type of AEO certificate

d) *Identify risks (which risks might influence the customs’ objectives)

Determine which of the potential risks are relevant for the particular operator, its business processes and supply chain.

- ❖ *IT enabler: Deploy business signal based on automated self-assessment (Digiscan)*

In this step, DutchTCA mainly uses the applicant’s AEO self-assessment summary compared with the actual information achieved from the “understanding business” step to address the risk indicators and corresponding points of attention. The self-assessment summary is based on the AEO guidelines, which can be automated assessed by the Digiscan tool. Digiscan deploys a rule based system, with which it is possible to identify cases with potential Tax & Customs risks using a rule based decision system. Risk indicators, risk description and points of attentions which should guide the customs officials as well as the operators themselves are indicated in the Digiscan. Under further development, the Digiscan may effectively reflect the company’s information systems and internal control maturity level, and thus it can be used by DutchTCA for further decision making and evaluation.

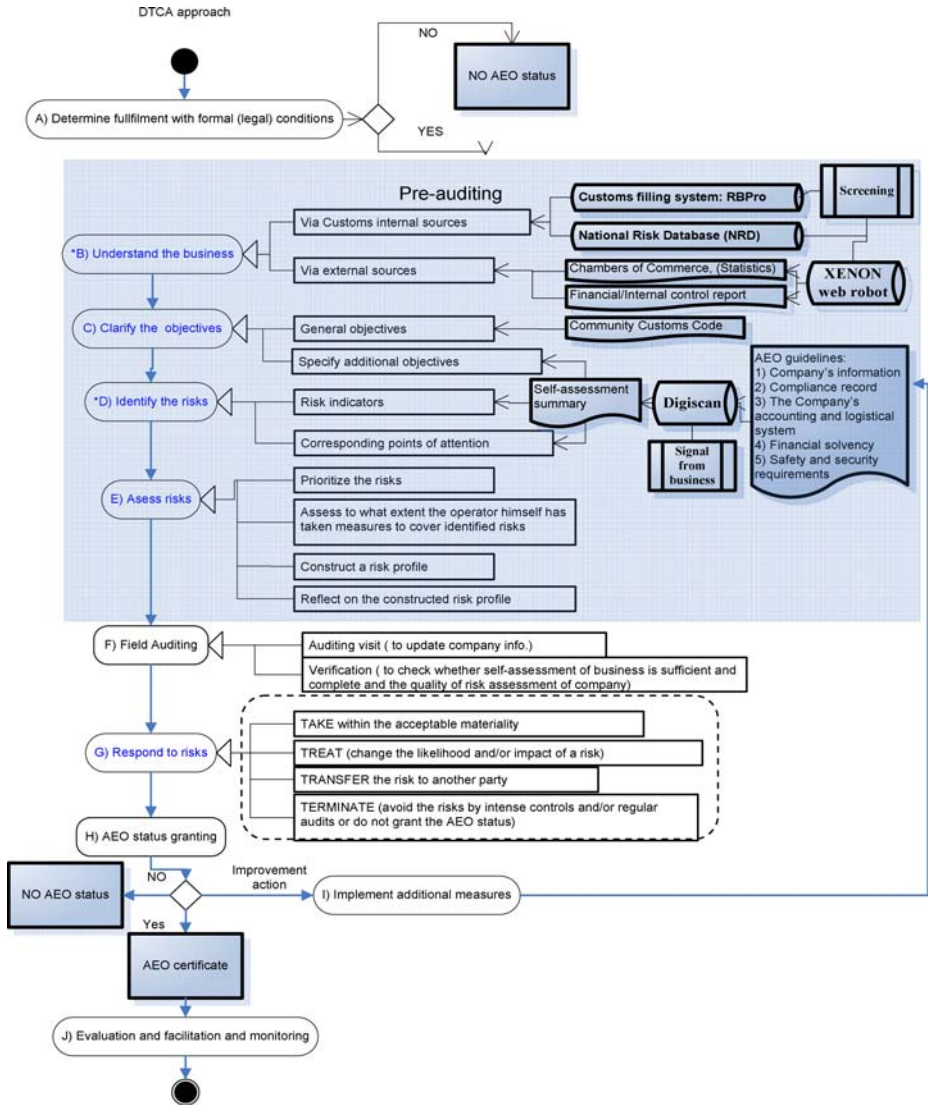


Fig. 4. DTCA AEO risk management approach

e) **Assess risks (which risks are the most significant) (not fully implemented by DutchTCA at the current stage yet)**

This step of the risk mapping approach is described by the AEO compact model [16] as:

- Prioritize the risks identified in step 3 through evaluation of the impact on customs objectives and the likelihood of the risk materializing.
- Assess to what extent the operator himself has taken measures to cover identified risks and in which way the operator prioritized the different types of risks.

- Construct a risk profile to provide a comprehensive picture of all significant risks.
- Reflect on the constructed risk profile

f) Field auditing (details skipped)

DutchTCA will undertake field auditing at the the company's offices. During this phase auditors determine whether the controls identified during pre-auditing have actually been implemented, and are operating effectively and in the manner described by the client.

g) Respond to risks: what to do about the (remaining) risks (details skipped)

Evaluate whether the AEO status is to be rejected or adjustments or improvements are to be made by the operator to cover the risk or to reduce it to an acceptable level.

h) AEO status granting (details skipped)

In this step DutchTCA make granting decisions based on the results from the auditing.

j) Evaluation, facilitation and monitoring (details skipped)

The status of an AEO is regularly evaluated and monitored by DutchTCA and relevant facilitations are given to the certified operator.

4 Conclusions

Information asymmetry has been studied extensively in economics research, but has received limited attention in the e-government field. In this paper we used the concept of asymmetric information, more specifically adverse selection, to analyze the relationship building between businesses and government regarding security and trade facilitation. In particular, we investigated the role of AEO certificates to build trust-based relationships between the Tax and Customs Administration and businesses. We argued that risk management can help to mitigate the problem of asymmetric information. In particular, we argued that IT plays in various ways an important role in this risk management to make the AEO certification process more efficient and effective. With effective signalling and screening, IT can mitigate the adverse selection problem for the G2B relationship building. A real life case of the AEO assessment in the Netherlands is presented in the paper, in which we showed how IT is included in the general risk management of the DutchTCA. The findings from this paper may provide valuable knowledge for the EU governments to further validate the AEO certification procedure, and provide a better understanding of the G2B relationship building.

Acknowledgements

The research of the first author was partially funded by the integrated project ITAIDE of the 6th Framework of the IST Programme.

References

1. EU Commission: Authorised economic operators—guidelines. Risk Management, Security and specific controls. DG Taxation and Customs Union, Brussels (June 29, 2007), http://ec.europa.eu/taxation_customs/resources/documents/customs/policy_issues/customs_security/AEO_guidelines_en.pdf
2. Akerlof, G.A.: The Market for “Lemons”: Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics* 84, 488–500 (1970)
3. Spence, M.: Job Market Signaling. *The Quarterly Journal of Economics* 87, 355–374 (1973)
4. Rothschild, M., Stiglitz, J.: Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information. *The Quarterly Journal of Economics* 90, 629–649 (1976)
5. Varian, H.R.: *Intermediate microeconomics: a modern approach*. WW Norton & Co., New York (2002)
6. Liu, J., Tan, Y.-H.: Moral hazard and G2B control procedures redesign. In: *Proceedings of the 9th Annual International Conference on Digital Government Research (DG.O 2008)*, Montreal, Canada. ACM International Conference Proceeding Series, vol. 289, pp. 421–422 (2008)
7. EU Parliament: Amending Council Regulation (EEC) No 2913/92 establishing the Community Customs Code. *Official Journal of the European Union* L 117/13 648/2005 (2005)
8. O’Reilly, C.A.: The use of information in organizational decision making: A model and some propositions. *Research in Organizational Behavior* 5, 103–139 (1983)
9. Feldman, M.S., March, J.G.: Information in Organizations as Signal and Symbol. *Administrative Science Quarterly* 26, 171–186 (1981)
10. Gertner, R., Gibbons, R., Scharfstein, D.: Simultaneous Signalling to the Capital and Product Markets. *The RAND Journal of Economics* 19, 173–190 (1988)
11. Eisenhardt, K.M.: Building theories from case study research. *The Academy of Management Review* 14, 532–550 (1989)
12. Yin, R.K.: *Case Study Research: Design and Methods*. Sage Publications Inc., Thousand Oaks (2003)
13. EU commission (Fiscalis Risk Analysis Project Group): *Risk Management Guide for tax administrations* (2006), http://ec.europa.eu/taxation_customs/resources/documents/taxation/tax_cooperation/gen_overview/Risk_Management_Guide_for_tax_administrations_en.pdf
14. Gutierrez, X., Hintsa, J.: Voluntary Supply Chain Security Programs: A Systematic Comparison. In: *The International Conference on Information Systems, Logistics and Supply Chain*, Lyon, France, May 15–17 (2006)
15. Davenport, T.H., Brooks, J.D.: Enterprise systems and the supply chain. *The Journal of Enterprise Information Management* 17, 8–19 (2004)
16. EU Commission: Authorised economic operators: The AEO COMPACT model. DG Taxation and Customs Union. In: Directorate-General, T.A.C.U. (ed.), vol. TAXUD/2006/1452. Brussels (June 13, 2006), http://ec.europa.eu/taxation_customs/resources/documents/customs/policy_issues/customs_security/AEO_compact_model_en.pdf